

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

12/14/2020

12/16/2002 - UPDATED

SUBJECT:

Multiple Vulnerabilities in SolarWinds Orion Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple Vulnerabilities have been discovered in SolarWinds Orion, the most severe of which could allow for arbitrary code execution. SolarWinds Orion is an IT performance monitoring platform that manages and optimizes IT infrastructure. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:

The Cybersecurity and Infrastructure Security Agency (CISA) released an alert detailing active exploitation of the SolarWinds Orion Platform software versions 2019.4 HF 5 through 2020.2 HF 1.

SYSTEMS AFFECTED:

- SolarWinds Orion Platform versions 2019.4 HF 5 through 2020.2 HF 1

December 16 – UPDATED SYSTEMS AFFECTED:

- ***SolarWinds Orion Platform versions prior to 2019.4 HF 6***
- ***SolarWinds Orion Platform versions prior to 2020.2.1 HF 2***

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

Multiple Vulnerabilities have been discovered in SolarWinds Orion, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A security vulnerability due to a define visual basic script (CVE-2020-14005)
- An HTML injection vulnerability (CVE-2020-13169)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

December 16 – UPDATED TECHNICAL SUMMARY:

SolarWinds has released the second hotfix patch for versions 2020.2.1 HF 2. SolarWinds has also published a FAQ page that includes answers to several important questions including how to check your systems for compromise and information for work arounds if you are not able to upgrade your system to the latest patch level.

<https://www.solarwinds.com/securityadvisory/faq>

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by SolarWinds to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privilege user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

SolarWinds:

<https://www.solarwinds.com/securityadvisory>

US-CERT:

<https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software>

FireEye:

<https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>

GitHub:

https://github.com/fireeye/sunburst_countermeasures
<https://gist.github.com/alert3/c9dcce5474e55f408c93c086c30cddb7>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14005>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13169>

December 16 – UPDATED REFERENCES:

SolarWinds:

<https://www.solarwinds.com/securityadvisory/faq>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>